

(19)



JAPANESE PATENT OFFICE

(1)

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **60062252 A**(43) Date of publication of application: **10.04.85**

(51) Int. Cl

H04L 9/02
G06K 19/00
G09C 1/00

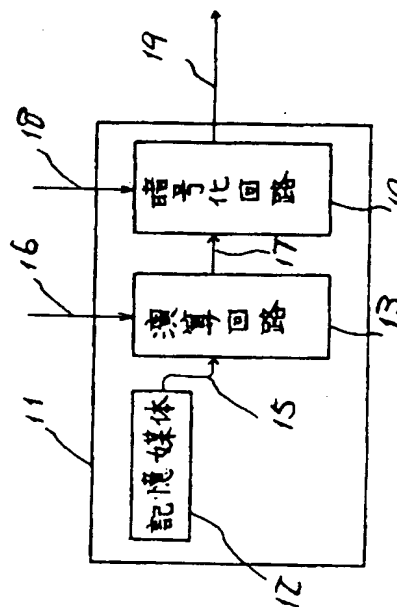
(21) Application number: **58169242**(71) Applicant: **TOSHIBA CORP**(22) Date of filing: **16.09.83**(72) Inventor: **UCHIHARA NAOSHI**(54) **CARD INCORPORATING ENCIPHERING CIRCUIT**

COPYRIGHT: (C)1985,JPO&Japio

(57) Abstract:

PURPOSE: To prevent the leakage of data and the generation of forgery without exposing a cipher key on a card by using a key code generated by an arithmetic circuit to encipher and output data to be sent through an enciphering circuit.

CONSTITUTION: The card 11 consists of a storage medium 12 stored with the number peculiar to the card, arithmetic circuit 13 which calculates the key code, enciphering circuit 14 which enciphers data, and signal transmission lines 15, 16@19. A random number R is inputted externally through the transmission line 16 firstly, and the key code K for enciphering is generated by a circuit 13 from this random number R and the number I peculiar to the card on the medium 12 and sent to the enciphering circuit 14. This circuit 14 inputs the original data to be sent through the transmission line 18 from the outside, and the key code is enciphered and outputted through the transmission line 19. This device is united in the card 11 and its internal state can not be checked externally at all.



EXAMINED PATENT PUBLICATION No. HEI-2-42261

Publication date: September 21, 1990

Title of the Invention: Card with cryptographic circuit
built therein and service center thereof

Publication No.: Sho 60-62252

Laid-open date: April 10, 1985

Application No. SHO-58-169242

Application date: Sept. 16, 1983,

Inventor: Naoshi Uchihira

c/o General Institute of Research, Tokyo Shibaura
Electric Co., Ltd.

No. 1, Komukae Toshiba-cho, Saiwai-ku, Kawasaki,
Kanagawa Pref.

Applicant: Tokyo Shibaura Electric Co., Ltd.

No. 72, Horikawa-cho, Saiwai-ku, Kawasaki,
Kanagawa Pref.

Agent: Norisuke Norichika, patent attorney, one other

Examiner: Teruo Naito

References:

Japanese Unexamined Patent Publication (Kokai) No. SHO 55-
55385 (JP, A), Japanese Unexamined Patent Publication (Kokai)
No. SHO 54-46447 (JP, A), Japanese Unexamined Patent
Publication (Kokai) No. SHO 54-148402 (JP, A)

Scope of Claim for a Patent

1. A card with cryptographic circuit built therein and a
service center thereof, comprising:

a controller for outputting a random number in
accordance with an ID code input thereto;

a card with a cryptographic circuit built therein,
including a storage medium for storing a preregistered unique
card number and the data to be transmitted, an arithmetic
circuit for generating a key code using the unique card
number output from the storage medium and the random number
output from said controller, and an encryption circuit for
encrypting and outputting said data to be transmitted using
the key code output from said arithmetic circuit;

a master card corresponding to each ID code, including a

storage medium for storing a preregistered unique card number and an arithmetic circuit for generating a key code using the unique card number output from the storage medium and the random number output from said controller; and

a decryption circuit for decrypting the cryptographic data output from the encryption circuit of the card having the cryptographic circuit built therein, using the key code output from the arithmetic circuit of the master card selected by said controller in accordance with the ID code input thereto;

characterized in that said controller, said master card and said decryption circuit are built in said service center.

Detailed Description of the Invention

[Technical Field of the Invention]

The present invention relates to a card with a cryptographic circuit built therein and a service center thereof for preventing the leakage and forgery of the contents transmitted by communication.

[Technical Background of the Invention and Problem Points thereof]

In recent years, in transmitting information (original data) to another party using an IC card having both the arithmetic function and the storage function, there has often occurred a case requiring the prevention of eavesdropping or malicious alteration of the transmitted contents. Conventionally, to cope with this problem, an external encryption device encrypts and transmits the original data using a key code (encryption key) generated by the IC card in accordance with the random number supplied from an external source.

In this method, however, the encryption key is provisionally exposed and therefore can be maliciously tampered with during the transmission of the encryption key to the encryption device. For example, it may happen that the encryption key transmitted from the IC card to the encryption circuit or the encrypted data transmitted from the encryption circuit is retrieved and the original data is

stolen by a third party using a decryption circuit commercially available. Also, the owner of an IC card having the original data stored in a storage medium can cut the connecting line for transmission of his original data to the encryption circuit and transmit other forged data. In this way, the contents of the conventional IC card are transmitted at the risk of leakage and forgery.

[Object of the Invention]

The object of the present invention is to provide a card and a service center thereof in which the leakage and forgery are prevented by preventing an encryption key from being exposed to the outside of the card.

[Summary of the Invention]

In this invention, a key code for encryption is generated by an arithmetic circuit based on the unique card number stored in a storage medium in the card and the random number input from a controller in the service center, and the data to be transmitted is output by being encrypted in an encryption circuit using the key code generated in the arithmetic circuit.

[Effects of the Invention]

According to this invention, the key code for encryption never leaks out but only the encrypted signal is exposed. Thus, the encrypted signal cannot be decrypted nor forged, thereby improving the practical advantage of preventing the information leakage.

[Embodiments of the Invention]

An embodiment of the present invention will be explained below with reference to the drawings.

Fig. 1 is a diagram showing an outline of this embodiment. A terminal 1 (hereinafter referred to as a service terminal) for receiving a service is connected by a signal transmission path 2 to a center (hereinafter referred to as a service center) 3 for managing the service. Individual information on the scope of available services is contained in the service terminal 1. This information is encrypted and sent by the card according to this invention to

the service center 3 without being directly exposed. The service center 3 decrypts the cryptograph by a method described later, and in response to a service request sent from the service terminal 1, determines whether the particular service request is included in the service scope and whether the service is to be provided or not.

Fig. 2 is a diagram showing a card according to an embodiment of the present invention. A card 11 is configured of a storage medium 12 for storing the number unique to the card, an arithmetic circuit 13 for calculating the key code, an encryption circuit 14 for performing encryption and signal transmission paths 15, 16, 17, 18, 19. First, a random number R is input from an external source through the transmission path 16. Based on the random number R and the unique card number I stored in the storage medium 12, an encryption key code K is generated in the arithmetic circuit 13 and sent to the encryption circuit 14. The encryption circuit 14 is supplied from an external source, through the transmission path 18, with the original data to be transmitted, and based on the key code, encrypts and outputs it through the transmission path 19. This device is integrated in the card 11, and the internal operation thereof is entirely invisible from outside. According to the embodiment shown in Fig. 2, the encryption circuit 14 is built in the card 11, and therefore the key code is not exposed. Thus, the leakage of the original data can be prevented.

Fig. 3 shows another embodiment of the invention, and is a diagram showing a general configuration of a service card 20 built in the service terminal. In the service card 20, the data input through the signal transmission path 18 of the card shown in Fig. 2 is built in the storage medium 21 as the contents stored in the card, and this storage medium 21 has stored therein the information S on the scope of the service. The service scope information S corresponds to, for example, the amount of deposit, credit line, etc. in a bank system application. Based on the number I unique to the card stored

in the storage medium 22 and the random number R sent from the signal transmission path 23, the arithmetic circuit 24 calculates the encryption key code K from the calculation rule $K = P(I, R)$ preventing leakage. Based on the encryption key code K, the service scope information S is encrypted by the encryption circuit 25 and transmitted outside through the signal transmission path 26 (the storage medium 24 and the storage medium 22 may be integrated with each other).

Fig. 4 is a detailed version of Fig. 1, and incorporates the embodiment of Fig. 3 as a part thereof. First, the card owner sets the service card 20 in the service terminal 1, and sends the ID code of the service card 20 (for example, the password for the CD card) to the service center 3 through the signal transmission path 27. Then, a controller 28 selects a master card 29 of the service card 20. (The service center holds the master cards of all the card owners.) The master card 29 is the service card 20, less the encryption circuit 25 and the storage medium 21. The same unique card number I is stored in the storage medium 22 and the storage medium 30. The arithmetic circuit 24 is also identical to the arithmetic circuit 31. In the process, the random number R is sent from the controller 28 through the signal transmission paths 23, 32 to the service card 20 and the master card 29 at the same time. Then, the arithmetic circuit 24 and the arithmetic circuit 31 generates the same encryption key code K according to the calculation rule $K = P(I, R)$. In the service card 20, the service scope information S providing the contents of the storage medium 21 is encrypted by the encryption circuit 25 based on the encryption key code K, and sent to the service center 3 through the signal transmission path 26. In the service center 3, the encrypted data is decrypted by the decryption circuit 33 based on the encryption key code K obtained from the master card 29 and thus the service scope information S can be restored. The service scope information S is stored in the storage medium 34. After that, in the case where a service request (for withdrawal of cash, for example) is received from the service terminal 1, the

controller 28 collates it with the service scope information S (outstanding amount of deposit) in the storage medium 34, and determines whether the related service is to be executed or not. According to this embodiment, the storage medium 21 as well as the encryption circuit 25 is built in the service card 20, and therefore the card owner cannot transmit other data to the encryption circuit. Thus forgery can be prevented. Also, the service scope information conventionally stored in the data base of the service center can be stored distributively in the service cards, and therefore the data storage space of the service center can be remarkably reduced.

Brief Description of the Drawings

Fig. 1 is a diagram showing an outline of an embodiment of the present invention, Fig. 2 a diagram showing a card according to an embodiment of the invention, Fig. 3 a diagram showing a card according to another embodiment of the invention, and Fig. 4 a detailed version of Fig. 1 incorporating the embodiment shown in Fig. 3.

1...Service terminal; 2...Signal transmission path;
3...Service center; 11...Card; 12, 21, 22, 30, 34...Storage medium; 13, 24, 31...Arithmetic circuit; 14, 25...Encryption circuit; 15, 16, 17, 18, 19, 23, 26, 27, 32...Signal transmission paths; 20...Service card; 28...Controller; 29...Master card; 33...Decryption circuit

8から乱数Rが信号伝送路23、32を通してサービスカード20とマスターカード29に同時に送られる。すると演算回路24と演算回路31では計算規則 $K=P(I, R)$ により同じ暗号キーコードKが発生される。サービスカード20では記憶媒体21の内容であるサービス範囲の情報Sを暗号キーコードKを基に暗号化回路25で暗号化し信号伝送路26を通してサービスセンタ3に送る。サービスセンタ3では暗号解読回路33において、マスターカード29から得られた暗号キーコードKを基に暗号を解読し、サービス範囲情報Sを復元することができる。そしてSを記憶媒体34に記憶させる。それ以後、サービス端末1からサービス要請（例えば現金引き出し）があつた場合、コントローラ28が記憶媒体34のサービス範囲情報S（預金高）と照らし合わせてそのサービスを実行するかしないかの判断を下す。この実施例によれば暗号化回路25ばかりでなく記憶媒体21もサービスカード20に内蔵されているので、カード所有者が他のデータを暗号化回路

へ送信することが不可能となり偽造を防げる。又、従来サービスセンタのデータベースに蓄えられていたサービス範囲情報を、各サービスカードの内部に分散させて記憶させることが出来るのでサービスセンタのデータ記憶領域を大幅に軽減することができる。

図面の簡単な説明

第1図は本発明の実施例の概要を示す図、第2図は本発明の一実施例によるカードを示す図、第3図は本発明の他の実施例のカードを示す図、第4図は第3図の実施例が組み込まれた第1図を詳細化した図である。

1……サービス端末、2……信号伝送路、3……サービスセンタ、11……カード、12、21、22、30、34……記憶媒体、13、24、31……演算回路、14、25……暗号化回路、15、16、17、18、19、23、26、27、32……信号伝送路、20……サービスカード、28……コントローラ、29……マスターカード、33……暗号解読回路。

Fig. 3
第3図

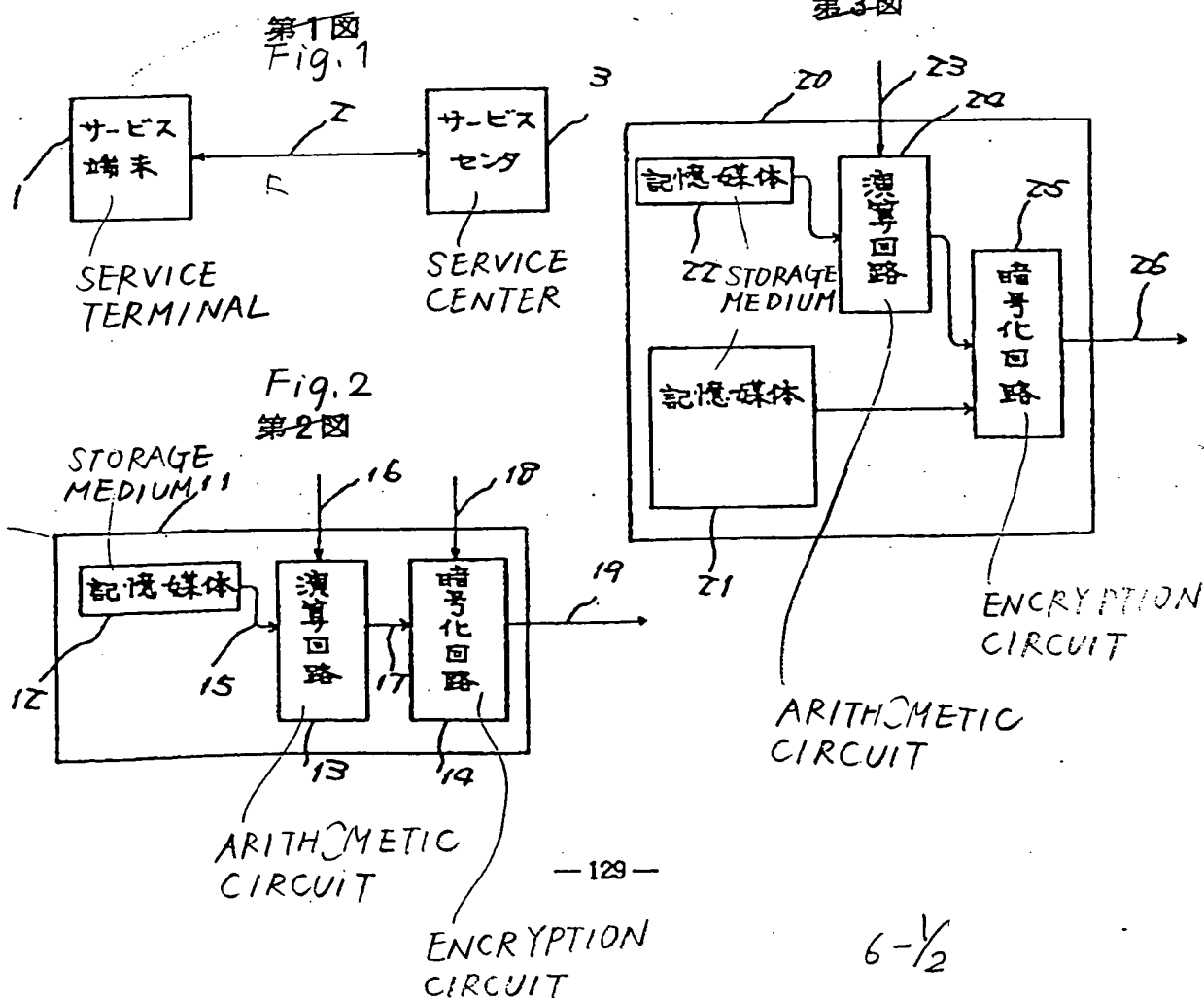
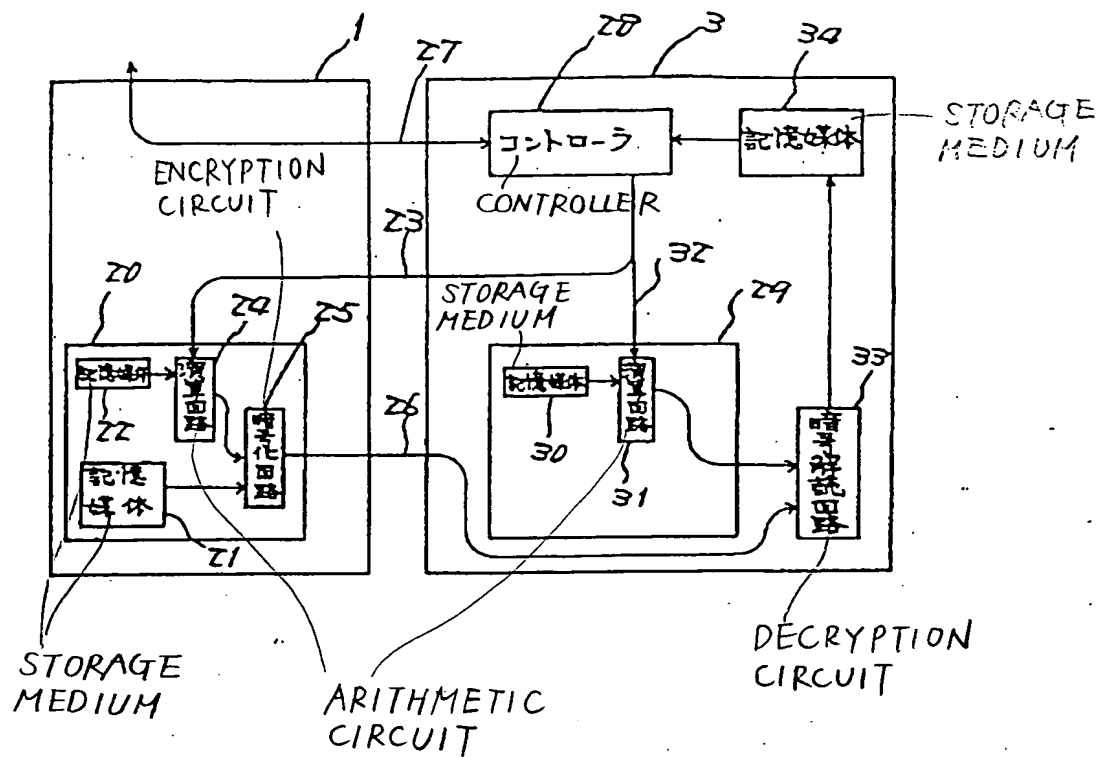


Fig. 4
第4図

⑨ 日本国特許庁(JP)

⑩ 特許出願公告 (1)

⑪ 特 許 公 報 (B2)

平2-42261

⑫ Int. Cl.⁵

識別記号

庁内整理番号

⑬ 公告 平成2年(1990)9月21日

H 04 L 8/06
G 06 K 19/073
G 09 C 1/00
H 04 L 9/14

3 1 0

7343-5B

6945-5K H 04 L 9/02
6711-5B G 06 K 19/00

Z
P

発明の数 1 (全4頁)

⑭ 発明の名称 暗号回路内蔵カード及びそのサービスセンター

⑮ 特 願 昭58-169242

⑯ 公 開 昭60-62252 (1)

⑰ 出 願 昭58(1983)9月16日

⑱ 昭60(1985)4月10日

⑲ 発 明 者 内 平 直 志 神奈川県川崎市幸区小向東芝町1 東京芝浦電気株式会社
総合研究所内

⑳ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

㉑ 代 理 人 弁 理 士 則 近 憲 佑 外 1 名

㉒ 審 査 官 内 藤 照 雄

㉓ 参 考 文 献 特 開 昭55-55385 (JP, A) 特 開 昭54-148402 (JP, A)

特 開 昭54-46447 (JP, A)

1

2

㉔ 特許請求の範囲

1 入力された識別コードに応じて乱数を出力するコントローラと、

予め登録されたカード固有番号及び送信すべきデータを記憶しておく記憶媒体、この記憶媒体から出力されたカード固有番号と前記コントローラから出力された乱数を用いてキーコードを発生する演算回路、この演算回路から出力されたキーコードを用いて前記送信すべきデータを暗号化して出力する暗号化回路、を備えた暗号回路内蔵カードと、

予め登録されたカード固有番号を記憶しておく記憶媒体、この記憶媒体から出力されたカード固有番号と前記コントローラから出力された乱数を用いてキーコードを発生する演算回路、を備え識別コードに夫々対応したマスターカードと、

前記入力された識別コードに従って前記コントローラより選択されたマスターカードの演算回路から出力されたキーコードを用いて前記暗号回路内蔵カードの暗号化回路より出力された暗号データを復号化する暗号解読回路とを具備し、

前記コントローラ、マスターカード及び暗号解読回路はサービスセンター内に組み込まれたこと

を特徴とする暗号回路内蔵カード及びそのサービスセンター。

発明の詳細な説明

〔発明の技術分野〕

5 本発明は通信における送信内容の漏洩、偽造を防ぐための暗号回路内蔵カード及びそのサービスセンターに関する。

〔発明の技術的背景とその問題点〕

近年、演算機能と記憶機能を合わせ持つICカードを用いて情報(原データ)を他へ送信する場合、この送信内容の盗聴、悪意による変更を防ぐ必要のある場合が生じる。従来は、このような目的から外から与えられる乱数に応じてICカードが発生するキーコード(暗号キー)を用いて、外部の暗号化装置が原データを暗号化して送信している。

ところがこの方式では、暗号キーが暗号化装置に送信される間に一端外部に出るため、そこでの何らかの悪意を持った操作が可能である。例えばICカードから暗号化回路へ送信された暗号キー、及び暗号化回路より送信された暗号化されたデータを外部の者が取り出し、市販されている暗号解読回路を使って原データを盗むことが可能であ

3

る。又、原データが記憶媒体に記憶されているICカードにおいては、このカードの所有者が自己の原データが暗号化回路へ送信される接続線をカットし、他の偽造データを送信することも可能である。このように従来のICカードにおいては送信内容の漏洩・偽造の危険性を伴うものであった。

【発明の目的】

本発明の目的は、暗号キーがカードの外部に出ることなく漏洩・偽造の発生を防ぐカード及びそのサービスセンターを提供することにある。

【発明の概要】

本発明はカード内において、記憶媒体に記憶されたカード固有番号とサービスセンター内のコントローラから入力された乱数とから演算回路で暗号化のキーコードを生成し、暗号化回路では演算回路で作られたキーコードを用いて送信すべきデータを暗号化して出力するものである。

【発明の効果】

本発明によれば、暗号化のキーコードは一切外部には漏れずに暗号化された信号だけが外部に出るので、暗号、信号を解釈・偽造することが出来なくなり、情報の漏洩を防ぐ意味で実用的利点が増大する。

【発明の実施例】

以下、本発明の一実施例につき図面を参照して説明する。

第1図は本実施例の概要を示す図である。サービスを受ける端末（以下サービス端末という）1は、サービスを管理するセンタ（以下サービスセンタという）3と信号伝送路2で結ばれている。サービスの受けられる範囲に関する個別な情報は、サービス端末1の中に存在するが、その情報は本発明によるカードにより直接外部に出ることなく暗号化されてサービスセンタ3に送られる。サービスセンタ3ではその暗号を後に述べる方式で解釈し、サービス端末1から送られてくるサービス要請に対し、そのサービス要請がサービス範囲内のものかを判断し、サービスを実行するかしないかの判断を下す。

第2図は本発明の一実施例によるカードを示す図である。カード11はこのカード固有の番号を記憶させた記憶媒体12とキーコードを計算する演算回路13と暗号化を行なう暗号化回路14と

4

信号伝送路15、16、17、18、19から構成される。まず、外部から伝送路16を通して乱数Rを入力し、この乱数Rと記憶媒体12のカード固有番号Iから演算回路13で暗号化のキーコードKを生成して暗号化回路14に送る。暗号化回路14は外部からの送信すべき原データを伝送路18から入力し、キーコードを基に暗号化し伝送路19を通して出力する。この装置はカード11内に一体化されていて、外部からは一切中の状態がわからないように作られる。この第2図の実施例によれば暗号化回路14がカード11に内蔵されているので、キーコードが外部に出る事が無くなり原データの漏洩を防げる。

第3図は本発明の他の実施例であり、サービス端末側に組み込まれるサービスカード20の概略構成図である。サービスカード20は第2図のカードの信号伝送路18を通して入力するデータをカード内部の記憶媒体21の記憶内容として組み込んだものであり、この記憶媒体21にはサービス範囲に関する情報Sが記憶されている。このサービス範囲情報Sとは例えば銀行システムに応用した場合の預金高、借入限度額等にあたる。記憶媒体22に記憶されているカード固有の番号Iと信号伝送路23から送られてくる乱数Rから、演算回路24が外部には漏れないある計算規則 $K = P(I, R)$ により暗号キーコードKを計算する。暗号キーコードKを基に、サービス範囲の情報Sを暗号化回路25で暗号化し、信号伝送路26を通して外部に伝達する。（尚、記憶媒体24と記憶媒体22は一体化されていてもよい。）

第4図は第1図を詳細化したもので第3図の実施例が一部として組み込まれている。先ずカード所有者はサービス端末1にサービスカード20をセットした後信号伝送路27を通してサービスセンタ3にサービスカード20の識別コード（たとえばCDカードの場合は暗証番号）を送る。するとコントローラ28がサービスカード20のマスタカード28を選択する。（サービスセンタ側にはカード所有者全てのマスタカードがある。）マスタカード29はサービスカード20から暗号化回路25と記憶媒体21を除いたもので記憶媒体22と記憶媒体30には同一のカード固有番号Iが記憶されており、演算回路24と演算回路31も同じものである。このときコントローラ2

5

6

8から乱数Rが信号伝送路23、32を通してサービスカード20とマスターカード29に同時に送られる。すると演算回路24と演算回路31では計算規則 $K=P(I, R)$ により同じ暗号キーコードKが発生される。サービスカード20では記憶媒体21の内容であるサービス範囲の情報Sを暗号キーコードKを基に暗号化回路25で暗号化し信号伝送路26を通してサービスセンタ3に送る。サービスセンタ3では暗号解読回路33において、マスターカード29から得られた暗号キーコードKを基に暗号を解読し、サービス範囲情報Sを復元することができる。そしてSを記憶媒体34に記憶させる。それ以後、サービス端末1からサービス要請（例えば現金引き出し）があつた場合、コントローラ28が記憶媒体34のサービス範囲情報S（預金高）と照らし合わせてそのサービスを実行するかしないかの判断を下す。この実施例によれば暗号化回路25ばかりでなく記憶媒体21もサービスカード20に内蔵されているので、カード所有者が他のデータを暗号化回路

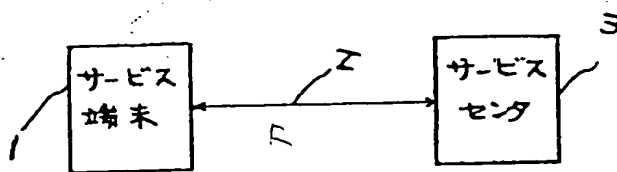
へ送信することが不可能となり偽造を防げる。又、従来サービスセンタのデータベースに蓄えられていたサービス範囲情報を、各サービスカードの内部に分散させて記憶させることが出来るのでサービスセンタのデータ記憶領域を大幅に軽減することができる。

図面の簡単な説明

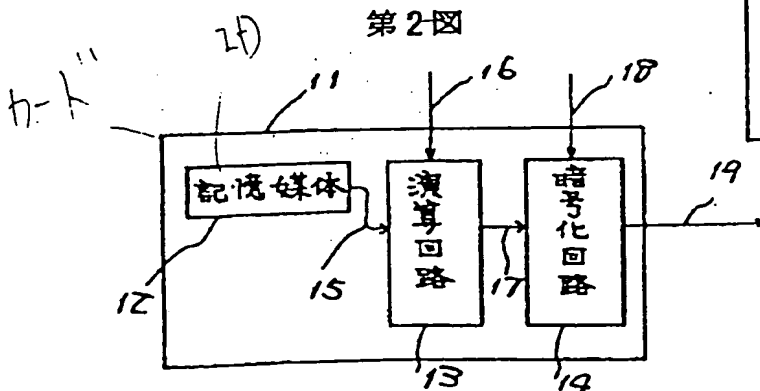
第1図は本発明の実施例の概要を示す図、第2図は本発明の一実施例によるカードを示す図、第3図は本発明の他の実施例のカードを示す図、第4図は第3図の実施例が組み込まれた第1図を詳細化した図である。

1……サービス端末、2……信号伝送路、3……サービスセンタ、11……カード、12、21、22、30、34……記憶媒体、13、24、31……演算回路、14、25……暗号化回路、15、16、17、18、19、23、26、27、32……信号伝送路、20……サービスカード、28……コントローラ、29……マスターカード、33……暗号解読回路。

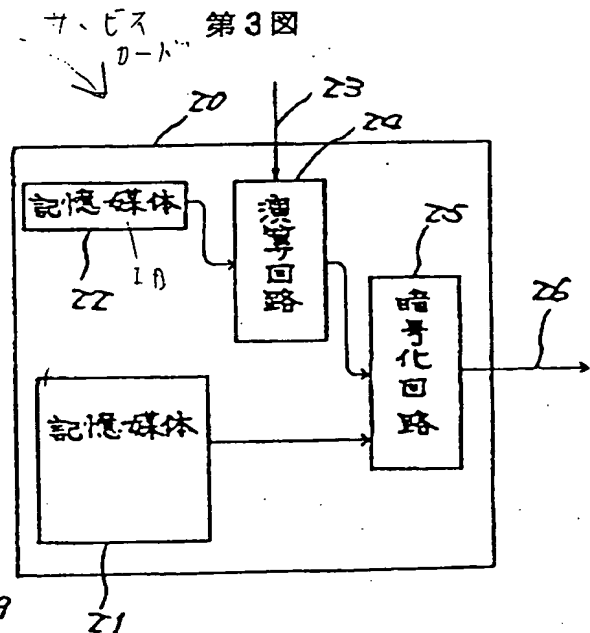
第1図



第2図



第3図



第4図

